Configurando um túnel IPsec - Cisco Router to Checkpoint Firewall 4.1

Contents

Introduction Prerequisites Requirements Componentes Utilizados Conventions Configurar Diagrama de Rede Configurações Verificar Troubleshoot Comandos para Troubleshooting Sumarização de rede Ponto de verificação Exemplo de saída de depuração Informações Relacionadas

Introduction

Esse documento demonstra como formar um túnel de IPsec com chaves pré-compartilhadas para unir duas redes privadas: a rede privada 192.168.1.x dentro do roteador Cisco e a rede privada 10.32.50.x dentro do Checkpoint Firewall.

Prerequisites

Requirements

Este exemplo de configuração pressupõe que o tráfego de dentro do roteador e de dentro do Ponto de verificação para a Internet (representado aqui pelas redes 172.18.124.x) flui antes de você iniciar a configuração.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco 3600 Router
- Software Cisco IOS® (C3640-JO3S56I-M), versão 12.1(5)T, SOFTWARE DE VERSÃO (fc1)

• Checkpoint Firewall 4.1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Consulte as <u>Convenções de Dicas Técnicas da Cisco para obter mais informações sobre</u> <u>convenções de documentos.</u>

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota:Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados neste documento.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Configurações

Este documento utiliza estas configurações.

- Configuração do roteador
- <u>Configuração do firewall do ponto de verificação</u>

Configuração do roteador

```
Configuração do Roteador Cisco 3600
Current configuration : 1608 bytes
!
version 12.1
no service single-slot-reload-enable
```

```
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
1
hostname cisco_endpoint
1
logging rate-limit console 10 except errors
1
ip subnet-zero
no ip finger
ip audit notify log
ip audit po max-events 100
1
!--- Internet Key Exchange (IKE) configuration crypto
isakmp policy 1
authentication pre-share
crypto isakmp key ciscorules address 172.18.124.157
1
!--- IPsec configuration crypto ipsec transform-set
rtpset esp-des esp-sha-hmac
crypto map rtp 1 ipsec-isakmp
set peer 172.18.124.157
set transform-set rtpset
match address 115
1
call rsvp-sync
cns event-service server
controller T1 1/0
1
controller T1 1/1
interface Ethernet0/0
ip address 172.18.124.35 255.255.250.240
ip nat outside
no ip mroute-cache
half-duplex
crypto map rtp
1
interface Ethernet0/1
ip address 192.168.1.1 255.255.255.0
ip nat inside
half-duplex
interface FastEthernet1/0
no ip address
shutdown
duplex auto
speed auto
ip kerberos source-interface any
ip nat pool INTERNET 172.18.124.36 172.18.124.36 netmask
255.255.255.240
ip nat inside source route-map nonat pool INTERNET
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.124.34
no ip http server
access-list 101 deny ip 192.168.1.0 0.0.0.255 10.32.50.0
0.0.0.255
access-list 101 permit ip 192.168.1.0 0.0.0.255 any
```

```
access-list 115 permit ip 192.168.1.0 0.0.0.255
10.32.50.0 0.0.0.255
access-list 115 deny ip 192.168.1.0 0.0.0.255 any
route-map nonat permit 10
match ip address 101
!
dial-peer cor custom
!
line con 0
transport input none
line aux 0
line vty 0 4
login
!
end
```

Configuração do firewall do ponto de verificação

Conclua estes passos para configurar o Firewall do Ponto de Verificação.

1. Como a duração padrão de IKE e IPsec difere entre os fornecedores, selecione Propriedades > Criptografia para definir a duração do ponto de verificação de acordo com os padrões da Cisco.O tempo de vida do IKE padrão da Cisco é de 86400 segundos (= 1440 minutos) e pode ser modificado por estes comandos:crypto isakmp policy #Nº de vida útilO tempo de vida do Cisco IKE configurável é de 60 a 86400 segundos. O tempo de vida padrão do Cisco IPsec é de 3600 segundos e pode ser modificado pelo comando crypto ipsec security-association lifetime seconds #.O tempo de vida do Cisco IPsec configurável é de 120 a 86400 segundos.

Properties Setup	×				
High Availability IP Pool NAT Acce Security Policy Traffic Control Services Authentication SYNDefender LDAP	ess Lists Desktop Security Log and Alert Security Servers Encryption ConnectControl				
SKIP Enable Exportable SKIP Change SKIP Session Key :					
Every or 120 Seconds (0 for infinity) Every 10485760 Bytes (0 for infinity)	Erom 100 To ffff				
IKE Renegotiate I <u>K</u> E Security Associations every Renegotiate I <u>P</u> SEC Security Associations every	1440 minutes 3600 seconds				
- WordPad 🛛 🛛 🗱 Command Prompt	RTPCPVPN - Check				

 Selecione Gerenciar > Objetos de rede > Novo (ou Editar) > Rede para configurar o objeto para a rede interna (chamada "cpinside") atrás do Ponto de controle. Isso deve concordar com a rede de destino (segunda) no comando Cisco access-list 115 permit ip 192.168.1.0 0.0.0.255 10.32.50.0 0.0.0.255. Selecione Interno em

Network Properties		X
General NAT		
<u>N</u> ame: cpin	side	
IP Address: 10.3	2.50.0	<u>G</u> et address
Net <u>M</u> ask: 255	255.255.0	
Comment:		Color:
Location: <u>Internal</u> <u>E</u>	xternal Sroadc	ast: wed O <u>D</u> isallowed
OK	Cancel	Help

3. Selecione Gerenciar > Objetos de rede > Editar para editar o objeto do ponto de extremidade RTPCPVPN Checkpoint (gateway) apontado pelo roteador Cisco no comando set peer 172.18.124.157.Selecione Interno em Local. Para Tipo, selecione Gateway. Em Módulos instalados, marque a caixa de seleção VPN-1 e FireWall-1 e também marque a caixa de seleção Estação de

Workstation Properties	×
General Interfaces SNMP N	AT Certificates VPN Authe
Name: RTPCPVPN	
IP Address: 172.18.124.157	<u>G</u> et address
Comment: Firewalled gatew	ay to internet
Location:	Туре:
● Internal O External	O <u>H</u> ost ⊙Gate <u>w</u> ay
Modules Installed	
VPN-1 & <u>F</u> ireWall-1	Version: 4.1 💌 <u>Get</u>
FloodGate-1	Version: 4.1
Compre <u>s</u> sion	Version: 4.1
Management Station	Color:
OK	Cancel Help

gerenciamento:

4. Selecione Gerenciar > Objetos de rede > Novo > Rede para configurar o objeto para a rede externa (chamada "inside_cisco") atrás do roteador Cisco.lsso deve concordar com a rede de origem (primeira) no comando Cisco access-list 115 permit ip 192.168.1.0 0.0.255 10.32.50.0 0.0.255.Selecione Externo em

Network Pro	perties			×
General N	AT)			
<u>N</u> ar	me: inside_cisco			
<u>I</u> P Addre	ss: 192.168.1.0		<u>G</u> et address	
Net <u>M</u> a	sk: 255.255.255.0			
<u>C</u> omme	ent:		Color:	•
C <u>I</u> ntern	al	Broadcast: <u>A</u> llowed	C <u>D</u> isallowed	
, [ОК	Cancel	Help]

5. Selecione Gerenciar > Objetos de rede > Novo > Estação de trabalho para adicionar um objeto para o gateway externo do roteador Cisco (chamado "cisco_endpoint"). Esta é a interface da Cisco à qual o comando crypto map name é aplicado.Selecione Externo em Local. Para Tipo, selecione Gateway.Observação: não marque a caixa de seleção VPN-

Workstation Properties	×				
General Interfaces SNMP NAT VPN					
<u>N</u> ame: <u>cisco_endpoint</u>					
IP Address: 172.18.124.35	<u>G</u> et address				
<u>C</u> omment:					
Location: O <u>I</u> nternal O <u>E</u> xternal	Type: ○ <u>H</u> ost ⓒ Gate <u>w</u> ay				
- Modules Installed					
VPN-1 & EireWall-1 Version: 4.1 🔽 Ge					
FloodGate-1	Version: 4.1				
Compre <u>s</u> sion	Version: 4.1				
Management Station	Color:				
ОК	Cancel Help				

- 1/FireWall-1.
- 6. Selecionar Manage > Network objetct > Edit para editar o ponto final do gateway do ponto de controle (chamado "RTPCPVPN") na guia VPN. Em Domain, selecione Other e, em seguida, selecione o lado interno da rede de ponto de controle (chamado "cpinside") a partir da lista suspensa. Sob esquemas de criptografia definidos, selecione IKE e clique em

Workstation Properties	
General Interfaces SNMP NAT Domain: ① Disabled ① Disabled ① Yalid Addresses(of Interfaces) ② Other: ① ① Disabled ▼ ③ Other: ▼ □ Exportable for SecuRemote	Certificates VPN Authe
Traffic Control Logging ■ Ium on Traffic Control Logging	
OK Cano	cel Help

- Altere as propriedades IKE da criptografia DES para concordar com estes comandos: crypto isakmp policy #encryption desObservação: a criptografia DES é o padrão, portanto, não é visível na configuração da Cisco.
- 8. Altere as propriedades de IKE para hashing SHA1 para concordar com estes comandos:crypto isakmp policy #hash shaObservação: o algoritmo de hash SHA é o padrão, portanto, ele não é visível na configuração da Cisco.Altere estas configurações:Desative o Modo assertivo.Verifique Suporta Sub-Redes.Marque Pre-Shared Secret em Authentication Method (Método de autenticação). Isso concorda com estes comandos:crypto isakmp policy #Pré-compartilhamento de

	General Interfaces SNMP NAT Certificates VPN Authe	¥
	KE Properties	×
	General	
	Key Negotiation Encryption Method(s): Hash Method: Image: DES Image: MD5 Image: CAST Image: SHA1	
	Authentication Method:	
	Supports Aggresive Mode Supports Subnets	
	OK Cancel Help	
autenticação		

9. Clique em **Editar segredos** para definir a chave pré-compartilhada para concordar com o comando **crypto isakmp key** *key*

Workstation Properties
General Interfaces SNMP NAT Certificates VPN Authe
IKE Properties
General
Shared Secret
Shared Secrets List:
Peer Name Shared Secret
<u>Edit</u>
<u>B</u> emove
OK Cancel
OK Cancel Help
OK Cancel Help

10. Selecione Gerenciar > Objetos de rede > Editar para editar a guia VPN "cisco_endpoint". Em Domain, selecione Other e, em seguida, selecione o interior da rede Cisco (chamado "inside_cisco"). Sob esquemas de criptografia definidos, selecione IKE e clique em

Workstation Properties	
General Interfaces SNMP NAT	VPN
Domain:	Encryption schemes defined:
© <u>D</u> isabled	Manual IPSEC
○ Valid Addresses(of Interfaces)	
• <u>O</u> ther:	D 🕅 SKIP
inside_cisco	
Exportable for SecuRemote	<u>E</u> dit
I ratitic Control Logging Turn on Traffic Control Logging	7
	2

- 11. Altere a criptografia DES das propriedades IKE para concordar com estes comandos: crypto isakmp policy #encryption desObservação: a criptografia DES é o padrão, portanto, não é visível na configuração da Cisco.
- 12. Altere as propriedades de IKE para hashing SHA1 para concordar com estes comandos:crypto isakmp policy #hash shaObservação: o algoritmo de hash SHA é o padrão, portanto, ele não é visível na configuração da Cisco.Altere estas configurações:Desative o Modo assertivo.Verifique Suporta Sub-Redes.Marque Pre-Shared Secret em Authentication Method (Método de autenticação). Isso concorda com estes comandos:crypto isakmp policy #Pré-compartilhamento de

Genera	I Interfaces SNMP NAT Certificate	es VPN Authe
KE Prop	perties 🚬	×
Genera	ц [°]	
	Key <u>N</u> egotiation Encryption Method(s): -	- <u>H</u> ash Method: -
	I I I I I I I I I I I I I I I I I I I	□ MD <u>5</u>
	D 🖾 3DES	✓ SHA1
	Authentication Method:	
	Pre-Shared Secret Ed	it <u>S</u> ecrets
	Public Key Signatures	onfigure
	□ Supports Aggresive <u>M</u> ode □ Supp	orts Su <u>b</u> nets
	OK Cancel	Help
autenticação		

13. Clique em **Editar segredos** para definir a chave pré-compartilhada para concordar com o comando da Cisco **crypto isakmp key**

	IKE Properties	×				
	General					
	Shared Secret	3				
	Shared Secrets List: Peer Name Shared Secret RTPCPVPN **** Edit Remove					
	OK Cancel					
address.	OK Cancel Help					

 Na janela Policy Editor, insira uma regra com Source e Destination como "inside_cisco" e "cpinside" (bidirecional). Ajustar Serviço=Qualquer, Ação=Criptografar e Rastreio=Longo.

1	RTPO	CPVPN - Check P	oint Policy Editor				_ 🗆 🗵
Ē	ile <u>E</u> di	it ⊻iew <u>M</u> anage	Policy <u>W</u> indow <u>H</u>	elp			
	- 5	🖪 🎗 🕒	E 💁 🕉 🕉	B. 🌮 🗽 😭	🗏 🖀 🖷 🖦	u, 🖡 🍽 📑	😓 🍸 🚯
	😫 Sec	urity Policy - Standard	🖥 🖶 Address Trans	slation - Standard 🛛 😿	Bandwidth Policy - St	andard	
	No.	Source	Destination	Service	Action	Track	In
ţ	1	👷 inside_cisco	👷 cpinside	Any	Encrypt	Long	6
ĮI.	•						•
F	or Help,	press F1		RTPC	PVPN Read	I/Write	1.

15. Clique no ícone **Criptografar** verde e selecione **Editar propriedades** para configurar políticas de criptografia no cabeçalho

Açao.				
rity Policy - Standard	🛃 Address Translation	- Standard 🐉 Band	dwidth Policy - Standard	
∼ FVV1 Host	∼ Ldap-Servers	😰 Idap	accept	
∼ FVV1 Host	∼ Logical-Servers	∼ load_agent	accept	
💂 inside_cisco 🔁 cpinside	💂 cpinside 💂 inside_cisco	Any	dit properties	hg .
		dest-unreach	Edit Encryption	
		icmp echo-reply	accept	am (
		icmp info-reply	drop	
Any	Any	icmp mask-reply	💆 🧲 reject	
•				•

16. Selecione IKE e, em seguida, clique em

-	Encryption Properties	×
	General Encryption schemes defined:	
tar	OK Cancel Help	

17. Na janela Propriedades de IKE, altere essas propriedades para concordar com as transformações do Cisco IPsec no comando **crypto ipsec transform-set rtpset esp-des esp-sha-hmac:**Em Transform, selecione Encryption + Data Integrity (ESP). O algoritmo de criptografia deve ser **DES**, a integridade dos dados deve ser **SHA1**, e o gateway de peer permitido deve ser o gateway de roteador externo (chamado "cisco_endpoint"). Click

IKE Properties	
General	
☐ransform: ⓒ Encryption + Data Integrit ⓒ Data Integrity Only (AH)	ty (ESP)
Encryption Algorithm:	DES
<u>D</u> ata Integrity	SHA1
Allowed Peer Gateway:	cisco_endpo 🔫
🔲 Use Perfect Forward Sec	recy
ок са	ancel Help

18. Depois de configurar o ponto de verificação, selecione **Política > Instalar** no menu Ponto de verificação para que as alterações entrem em vigor.

Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração está

funcionando adequadamente.

A <u>Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados</u> <u>comandos show.</u> Use a OIT para exibir uma análise da saída do comando show.

- show crypto isakmp sa Exibir todas as associações de segurança (SAs) IKE atuais em um peer.
- show crypto ipsec sa Exibir as configurações usadas pelas SAs atuais.

Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Comandos para Troubleshooting

Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.

- debug crypto engine Exibe mensagens de depuração sobre mecanismos de criptografia, que executam criptografia e descriptografia.
- debug crypto isakmp Exibe mensagens sobre eventos de IKE.
- debug crypto ipsec Exibe eventos de IPSec.
- clear crypto isakmp Limpa todas as conexões IKE ativas.
- clear crypto sa Limpa todas as SAs IPsec.

Sumarização de rede

Quando várias redes internas adjacentes são configuradas no domínio de criptografia no ponto de verificação, o dispositivo pode resumi-las automaticamente em relação ao tráfego interessante. Se o roteador não estiver configurado para corresponder, o túnel provavelmente falhará. Por exemplo, se as redes internas de 10.0.0.0 /24 e 10.0.1.0 /24 estiverem configuradas para serem incluídas no túnel, elas podem ser resumidas em 10.0.0.0 /23.

Ponto de verificação

Como o rastreamento foi definido para Long na janela Policy Editor, o tráfego negado deve aparecer em vermelho em Log Viewer. É possível obter mais depuração detalhada com:

C:\WINNT\FW1\4.1\fwstop C:\WINNT\FW1\4.1\fw d -d e em outra janela:

C:\WINNT\FW1\4.1\fwstart

Observação: esta foi uma instalação do Microsoft Windows NT.

Emita estes comandos para limpar SAs no ponto de verificação:

fw tab -t IKE_SA_table -x
fw tab -t ISAKMP_ESP_table -x
fw tab -t inbound_SPI -x
fw tab -t ISAKMP_AH_table -x

Responda sim na janela Tem certeza? prompt.

Exemplo de saída de depuração

Configuration register is 0x2102

```
cisco_endpoint#debug crypto isakmp
Crypto ISAKMP debugging is on
cisco_endpoint#debug crypto isakmp
Crypto IPSEC debugging is on
cisco_endpoint#debug crypto engine
Crypto Engine debugging is on
cisco_endpoint#
20:54:06: IPSEC(sa_request): ,
  (key eng. msg.) src= 172.18.124.35, dest= 172.18.124.157,
    src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    dest_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
   protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xA29984CA(2727969994), conn_id= 0, keysize= 0, flags= 0x4004
20:54:06: ISAKMP: received ke message (1/1)
20:54:06: ISAKMP: local port 500, remote port 500
20:54:06: ISAKMP (0:1): beginning Main Mode exchange
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) MM_NO_STATE
20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I) MM_NO_STATE
20:54:06: ISAKMP (0:1): processing SA payload. message ID = 0
20:54:06: ISAKMP (0:1): found peer pre-shared key matching 172.18.124.157
20:54:06: ISAKMP (0:1): Checking ISAKMP transform 1 against priority 1 policy
20:54:06: ISAKMP:
                      encryption DES-CBC
20:54:06: ISAKMP:
                      hash SHA
                     default group 1
20:54:06: ISAKMP:
20:54:06: ISAKMP:
                     auth pre-share
20:54:06: ISAKMP (0:1): atts are acceptable. Next payload is 0
20:54:06: CryptoEngine0: generate alg parameter
20:54:06: CRYPTO_ENGINE: Dh phase 1 status: 0
20:54:06: CRYPTO_ENGINE: Dh phase 1 status: 0
20:54:06: ISAKMP (0:1): SA is doing pre-shared key authentication
  using id type ID_IPV4_ADDR
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) MM_SA_SETUP
20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I) MM_SA_SETUP
20:54:06: ISAKMP (0:1): processing KE payload. message ID = 0
20:54:06: CryptoEngine0: generate alg parameter
20:54:06: ISAKMP (0:1): processing NONCE payload. message ID = 0
20:54:06: ISAKMP (0:1): found peer pre-shared key matching 172.18.124.157
20:54:06: CryptoEngine0: create ISAKMP SKEYID for conn id 1
20:54:06: ISAKMP (0:1): SKEYID state generated
20:54:06: ISAKMP (1): ID payload
       next-payload : 8
                    : 1
       type
       protocol
                    : 17
       port
                    : 500
       length
                     : 8
20:54:06: ISAKMP (1): Total payload length: 12
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) MM_KEY_EXCH
20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I) MM_KEY_EXCH
```

```
20:54:06: ISAKMP (0:1): processing ID payload. message ID = 0
20:54:06: ISAKMP (0:1): processing HASH payload. message ID = 0
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ISAKMP (0:1): SA has been authenticated with 172.18.124.157
20:54:06: ISAKMP (0:1): beginning Quick Mode exchange, M-ID of 1855173267
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) QM_IDLE
20:54:06: CryptoEngine0: clear dh number for conn id 1
20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I) QM_IDLE
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ISAKMP (0:1): processing HASH payload. message ID = 1855173267
20:54:06: ISAKMP (0:1): processing SA payload. message ID = 1855173267
20:54:06: ISAKMP (0:1): Checking IPSec proposal 1
20:54:06: ISAKMP: transform 1, ESP_DES
20:54:06: ISAKMP: attributes in transform:
20:54:06: ISAKMP: encaps is 1
                    SA life type in seconds
SA life duration (basic) of 3600
SA life type in kilobytes
20:54:06: ISAKMP:
20:54:06: ISAKMP:
20:54:06: ISAKMP:
20:54:06: ISAKMP:
                     SA life duration (VPI) of 0x0 0x46 0x50 0x0
20:54:06: ISAKMP: authenticator is HMAC-SHA
20:54:06: validate proposal 0
20:54:06: ISAKMP (0:1): atts are acceptable.
20:54:06: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) dest= 172.18.124.157, src= 172.18.124.35,
   dest_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
   src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
   protocol= ESP, transform= esp-des esp-sha-hmac ,
   lifedur= 0s and 0kb,
   spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
20:54:06: validate proposal request 0
20:54:06: ISAKMP (0:1): processing NONCE payload. message ID = 1855173267
20:54:06: ISAKMP (0:1): processing ID payload. message ID = 1855173267
20:54:06: ISAKMP (0:1): processing ID payload. message ID = 1855173267
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ipsec allocate flow 0
20:54:06: ipsec allocate flow 0
20:54:06: ISAKMP (0:1): Creating IPSec SAs
20:54:06:
                 inbound SA from 172.18.124.157 to 172.18.124.35
       (proxy 10.32.50.0 to 192.168.1.0)
20:54:06:
                has spi 0xA29984CA and conn_id 2000 and flags 4
                 lifetime of 3600 seconds
20:54:06:
                 lifetime of 4608000 kilobytes
20:54:06:
20:54:06:
                 outbound SA from 172.18.124.35 to 172.18.124.157
   (proxy 192.168.1.0 to 10.32.50.0)
20:54:06: has spi 404516441 and conn_id 2001 and flags 4
20:54:06:
                 lifetime of 3600 seconds
                 lifetime of 4608000 kilobytes
20:54:06:
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) QM_IDLE
20:54:06: ISAKMP (0:1): deleting node 1855173267 error FALSE reason ""
20:54:06: IPSEC(key_engine): got a queue event...
20:54:06: IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 172.18.124.35, src= 172.18.124.157,
    dest_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    src_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
   protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xA29984CA(2727969994), conn_id= 2000, keysize= 0, flags= 0x4
20:54:06: IPSEC(initialize_sas): ,
  (key eng. msg.) src= 172.18.124.35, dest= 172.18.124.157,
    src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    dest_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
   protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
```

```
spi= 0x181C6E59(404516441), conn_id= 2001, keysize= 0, flags= 0x4
20:54:06: IPSEC(create_sa): sa created,
  (sa) sa_dest= 172.18.124.35, sa_prot= 50,
   sa_spi= 0xA29984CA(2727969994),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 2000
20:54:06: IPSEC(create_sa): sa created,
  (sa) sa_dest= 172.18.124.157, sa_prot= 50,
    sa_spi= 0x181C6E59(404516441),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 2001
cisco_endpoint#sho cry ips sa
interface: Ethernet0/0
   Crypto map tag: rtp, local addr. 172.18.124.35
   local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.32.50.0/255.255.255.0/0/0)
   current_peer: 172.18.124.157
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 14, #pkts encrypt: 14, #pkts digest 14
    #pkts decaps: 14, #pkts decrypt: 14, #pkts verify 14
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0,
    #pkts decompress failed: 0, #send errors 1, #recv errors 0
    local crypto endpt.: 172.18.124.35, remote crypto endpt.: 172.18.124.157
    path mtu 1500, media mtu 1500
    current outbound spi: 181C6E59
     inbound esp sas:
     spi: 0xA29984CA(2727969994)
       transform: esp-des esp-sha-hmac ,
       in use settings ={Tunnel, }
       slot: 0, conn id: 2000, flow_id: 1, crypto map: rtp
 --More--
                         sa timing: remaining key lifetime (k/sec):
    (4607998/3447)
       IV size: 8 bytes
       replay detection support: Y
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
     spi: 0x181C6E59(404516441)
       transform: esp-des esp-sha-hmac ,
       in use settings ={Tunnel, }
       slot: 0, conn id: 2001, flow_id: 2, crypto map: rtp
       sa timing: remaining key lifetime (k/sec): (4607997/3447)
       IV size: 8 bytes
       replay detection support: Y
     outbound ah sas:
     outbound pcp sas:
cisco_endpoint#show crypto isakmp sa
                                          conn-id slot
                        state
   dst
                src
172.18.124.157 172.18.124.35 QM_IDLE
                                             1
                                                      0
```

```
\texttt{cisco\_endpoint} \texttt{\texttt{#exit}}
```

Informações Relacionadas

- <u>Negociação IPsec/Protocolos IKE</u>
- <u>Configuração da segurança de rede IPSec</u>
- <u>Configurando o protocolo de segurança do intercâmbio chave de Internet</u>
- Suporte Técnico e Documentação Cisco Systems